

## UNITED STATES DISTRICT COURT

FILED

JAN 29 2020

U.S. DISTRICT COURT  
EASTERN DISTRICT OF MO  
ST. LOUIS

for the

Eastern District of Missouri

In the Matter of the Search of

IN THE MATTER OF THE SEARCH OF INFORMATION  
information associated with Facebook Inc., profile Cash Bandicoot  
(ID: 100001392692564), stored at premises operated by Facebook,  
Inc., in Menlo Park, California.

Case No. 4:20 MJ 6025 PLC

## APPLICATION FOR A SEARCH WARRANT

I, Matthew Baughn, a federal law enforcement officer or an attorney for the government  
request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

Facebook profile of Cash Bandicoot (ID: 100001392692564)

located in the NORTHERN District of CALIFORNIA, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

## Code Section

18:1951; 2119; 924(c); and 922

## Offense Description

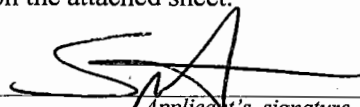
Hobbs Act Robbery; Carjacking; Possession of a firearm in furtherance of a crime of violence;  
and felon in possession of a firearm

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

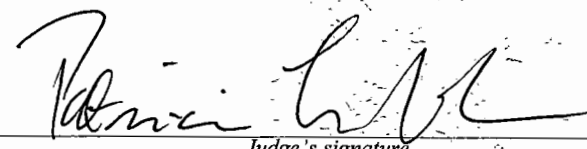
☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested  
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature  
 Matthew Baughn, SA, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: January 29, 2020City and state: St. Louis, MO
  
 Judge's signature

Honorable Patricia L. Cohen, U.S. Magistrate Judge

Printed name and title

AUSA: THOMAS J. MEHAN, #28958MO

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF	)	
INFORMATION ASSOCIATED WITH	)	No. 4:20 MJ 6025 PLC
FACEBOOK USER <b>Cash Bandicoot (ID:</b>	)	
<b>100001392692564)</b> THAT IS STORED AT	)	
PREMISES CONTROLLED BY	)	FILED UNDER SEAL
FACEBOOK, INC.	)	

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent S. Matthew Baughn, FBI, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. The requested warrant would require Facebook to disclose to the United States records and other information in its possession, pertaining to the subscriber or customer associated with the user ID as further described in attachment B.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510 of Title 18, United States Code, and I am empowered by law to conduct investigations of and to make arrests for the offenses enumerated in Title 18, United States Code, Section 2516. I have been employed as a SA of the FBI since 2010. I am currently

assigned to a squad responsible for the investigation of crimes of violence. Through my training and experience, I am familiar with the debriefing of cooperating witnesses and/or other sources of information and methods of searching locations where illegal drugs, firearms, instruments of money laundering, and evidence of other crimes may be found. I have been trained in and have experience conducting surveillance.

3. Information in this affidavit is based upon my own investigation and that of several Federal and local experienced law enforcement investigators with whom I am working. The statements contained in this affidavit are based in part on information and written reports provided by other law enforcement investigators; information gathered from provided from cooperating witnesses, surveillance and on my experience and background and the experience and background of other law enforcement officers. As part of the investigation, described in this affidavit, I have reviewed public and law enforcement records and talked with or reviewed reports of other law enforcement officers. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1951 (hobbs act robbery), 2119 (carjacking), Section 924(c) (possession of a firearm in connection with a crime of violence), and 922, (unlawful possession of a firearm) have been committed by WILLIE FRAZIER and others known and unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

5. The statements contained in this Affidavit are based in part on information provided by St. Louis Metropolitan Police Department ("SLMPD") officers, my own investigation, and written and oral reports about this and other investigations that I have received, directly or indirectly, from various local law enforcement agencies. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that — has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

### **LOCATION TO BE SEARCHED**

7. The location to be searched is:

Cash Bandicoot (ID: 100001392692564) (hereinafter referred to as "Subject Account(s)") with Facebook, Inc., located at 1601 Willow Road, Menlo Park, CA 94025, further described in Attachment A. The items to be reviewed and seized by the United States are described in Part II of Attachment B.

### **BACKGROUND RELATING TO FACEBOOK**

8. The Internet is in part a computer communications network using interstate and foreign telephone and communication lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive data and image files.

9. An "Internet Protocol" (IP) address is a unique series of numbers, separated by a period, that identifies each computer using, or connected to, the Internet over a network. An IP address permits a computer (or other digital device) to communicate with other devices via the Internet. The IP addresses aids in identifying the location of digital devices that are connected to the Internet so that they can be differentiated from other devices. As a mailing address allows a sender to mail a letter, a remote computer uses an IP address to communicate with other computers.

10. An "Internet Service Provider" (ISP) is an entity that provides access to the Internet to its subscribers.

11. The term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

12. Facebook is a business and company that operates as a remote computing service, a provider of electronic communications services through ISPs. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

13. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.



14. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and creator of the group. Facebook uses the term “Group Contact Info” to describe the contact information for the group’s creator and administrator, as well as the current status of the group profile page.

15. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

16. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Depending on the user’s privacy settings, Facebook may also obtain and store the physical location of the user’s device(s) as they interact with the Facebook service on those device(s). Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

17. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

18. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (*i.e.*, label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. Facebook allows users to edit or delete comments on their own profile pages, and users can adjust their profile settings to allow them to pre-approve comments on their own profile pages.

19. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

20. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

21. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

22. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

23. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

24. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

25. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.



26. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

27. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications. When a given Facebook account is deleted, Facebook retains certain information relating to that account for some period of time, including user identity information, IP logs, and other data. Even if a given user deletes data, Facebook stores such data for extended periods of time on Facebook’s servers.

28. Messages, photos, audio videos, and other records stored on Facebook server by a subscriber may not necessarily be located in the subscriber’s home/work computer. The subscriber or user may store data on Facebook servers for which there is insufficient storage space in the subscriber’s computer and/or which he/she does not wish to maintain in the computer at his/her residence or employment. A search of the files in the computer at the

subscriber's residence or place of employment will not necessarily uncover the files that the subscriber has stored on the Facebook server. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account application.

29. By their very nature, websites, social networking accounts, and internet-based applications described herein are kept and stored in computers and electronic-memory devices by the host companies, in addition to or in lieu of hard-copy versions of this data. Because such evidence is stored electronically, the data and evidence of the crimes described herein may be stored and be present for long periods of time.

30. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

31. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be

evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

32. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

**PROBABLE CAUSE**

33. On 1/8/2018, telephone number 314-414-3920 place an order with Dominos Pizza, located at 7259 Manchester Road, Maplewood, MO 63143. The order was for delivery to 2221 Benton Terrace, 2221 Benton Terrace, St. Louis, MO 63139.

34. When the delivery driver, KB, walked to the door of the 2221 Benton Terrace, he realized it was a vacant apartment. He returned to his vehicle to call the customer at 314-414-3920 from his personal cellular phone, 618-558-7471. While sitting in his 2018 maroon Chevy Cruz, he observed two male suspects walking towards him from the gangway of the east of 2221 Benton Terrace. The two suspects approached him and produced black pistols and pointed them at him. The suspects demanded his money, the pizzas, his cellular phone, and the keys to his vehicle. Then they ordered him to run away and he ran west from this location to 2131 Franz Park Lane, where he contacted the SLMPD. He described the suspects as two males, in their early to mid-twenties, one wearing a camouflage jacket and the other wearing a gray hooded sweatshirt.

35. The subscriber for the target phone, 314-414-3920, resolved to a VOIP account as follows:

Username: shaunking357  
Email: shaunking357@gmail.com  
Assigned/Unassigned dates: 10/28/2017 - currently assigned (as of 3/13/2018)

36. A search for email address shaunking357@gmail.com resolved to Facebook account "Troub Ril Coley Williams" (FB# 100016702819212). A preservation letter for this account was sent to Facebook on 3/13/2018.

37. Review of the call log for VOIP phone number 314-414-3920 confirmed this number called the Dominos location shortly before the carjacking/robbery. The log also

confirmed victim called this number from his person cellular phone immediately before the carjacking.

38. A more detailed review of the log revealed VOIP phone number 314-414-3920 made calls to telephone number 314-755-4887. This T-Mobile number resolved in to Alvin Nashaun Green.

39. A review of Green's photos in Crime Matrix identified Green as a possible match to the photos on the Facebook page of "Troub Ril Coley Williams."

40. A search for Green further revealed he was taken into custody by the St. Louis County Police around 2/28/2018. When Green was taken into custody, he provided consent for detectives to search his cellular phone.

41. The image of Green's phone included a list of User Accounts on the phone, TextNow was listed with the username shaunking357, email shaunking357@gmail.com, and phone number 314-414-3920. The application was installed on 10/24/2017. The Chats included texts and calls using the TextNow application. Included in this list was a missed call on 1/9/2018 at 3:51:11 AM (UTC+0) from 618-558-7471. (NOTE: 618-558-7471 was identified as the victim's cellular phone that was taken the night of the carjacking)

42. On August 20, 2019, Green was interviewed with his attorney present and advised the following:

Green, Willie Frazier, and Darrin Cody were all together on 1/8/2018 in Green's black 4 door Suzuki sedan when Frazier and Cody came up with the plan to rob a Domino's delivery driver. Green could not recall who made the call to Dominos, but thought it may have been Frazier using Green's cellular phone. There was some



discussion about using an application to mask the phone number calling Domino's when they placed the order.

After the pizza was ordered, Green, Frazier, and Cody all drove to a parking lot behind the delivery location to wait in Green's vehicle for the driver to arrive. When the driver called Green's phone, Frazier stayed in Green's vehicle while Green and Cody, both armed with loaded pistols, walked around the side of the building and approached the driver. Green and Cody ordered the driver to the ground and held him at gunpoint while Cody searched his pockets for his money, phone, and car keys. Cody then told the victim to run away and walked towards the victim's vehicle, which Green described as a new model burgundy sedan. While Cody entered the victim's vehicle, Green went back to his vehicle and noticed Frazier was now in the driver's seat. Frazier and Green pulled around the building and pulled up alongside Cody, who was driving the victim's vehicle. Frazier and Cody told Green to get in the victim's car with Cody, but Green refused. Frazier and Green stayed in Green's vehicle, while Cody went in another direction in the victim's vehicle.

A short time later, Frazier and Cody were in contact. Frazier told Green they had to go pick up Cody who had ditched the victim's vehicle in the Brentwood area. Frazier and Green drove in Green's vehicle to a hotel near the Target store in Brentwood.

After picking up Cody, the group traveled to an apartment complex in Brentwood where Cody said he ditched the victim's vehicle. When Green, Frazier, and Cody located the victim's vehicle in the apartment complex, Green noticed Cody had already removed the Domino's sign from the vehicle. (NOTE: Green was again shown a map of the

Brentwood area and identified the apartment complex behind the Brentwood Square strip mall as the location where Cody ditched the victim's vehicle.)

Frazier or Cody then drove the victim's vehicle somewhere in downtown St. Louis and left it there. Frazier later told Green he sold the vehicle to someone who wrecked it. Frazier received cash and drugs for the sale of the vehicle.

43. On October 1, 2019, SLMPD provided an image of a phone Frazier identified as his. A review of this device identified logins to multiple accounts. The phone was used to login accounts belonging to Frazier, but also accessed accounts that appear to belong to Cody, including email address [darrincody18@gmail.com](mailto:darrincody18@gmail.com) and Facebook username darrin.cody.3 (vanity name: A'hmiya Shooter) and Facebook username bpgehoe (vanity name: Cash Bandicoot, ID: 100001392692564). Based upon this activity, investigators believe Cody and Frazier both utilized this phone at various times to log into Facebook and other accounts.

44. A comparison of known photographs of Cody and the profile pictures of the Facebook account of Cash Bandicoot lead investigators to believe Cody is the user of Facebook account Cash Bandicoot, ID: 100001392692564.

45. Included in the images from this device were two screenshots of a Facebook messenger conversations. The first screenshot was taken at approximately 12:04am on January 9, 2018 and included a photograph of a maroon Chevy Cruz consistent with the victim's vehicle. The second screenshot was taken at approximately 1:30am and includes a different image of a maroon Chevy Cruz consistent with the victim's vehicle. This second screenshot was sent to Facebook user "Deonte." In this second screenshot, the message includes "Chevy cruise."

46. A search of Frazier's Facebook Account Willie Frazier (ID: 100025570087807) did not show any friends with the name "Deonte" or the associated profile picture. A search of

Cody's Facebook page, Cash Bandicoot (ID: 100001392692564), identified a friend with the name "Deonte Ingram" (username depeeboyy.deonte) and a profile image matching the one in the second screenshot sent at 1:30am over Facebook messenger mentioned above.

47. Based upon images on Frazier's phone, investigators believe Cody used his FB account to send images of the carjacked Chevy Cruz on 1/9/2018 via Facebook Messenger to the Facebook account "Deonte Ingram."

48. From my knowledge, training and experience, as well as discussions I have had with other agents and personnel familiar with computer-related investigations, I know that it is common for individuals engaged in the criminal activities described herein to use social networking sites such as Facebook to communicate with one another and facilitate their criminal activities. Such communications and the facilitation of criminal activities include the use of these applications and electronic and stored data that would identify and describe: (a) other co-conspirators, aiders, and abettors who are participating in the illegal activities as well as the nature and scope of the illegal activities; (b) identify dates and locations where illegal activity has taken place or may take place in the future; (c) discussions concerning planning, operations, the transfer of information, concerning the illegal activities described herein as well as sharing photographs, videos, documents, and files, (d) financial transactions and monetary transfers used to facilitate and continue criminal activities as well as the existence and location of records, bank accounts, and businesses pertaining to those activities; (e) sales and purchases of equipment, materials, and goods used to aid the co-conspirators in their endeavors as well as the location and use of assets accumulated; (f) travel, safe-houses, and locations where goods, materials and personnel stay or are kept; and (g) the existence of other communication facilities, including

telephones, computers, e-mail and other electronic accounts used to by co-conspirators to communicate.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

49. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the United States copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

**CONCLUSION**

50. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Facebook. Because the warrant will be served on Facebook, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

51. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

52. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution,

destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

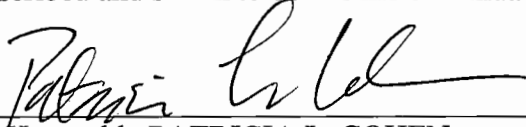
Respectfully submitted,



---

S. MATTHEW BAUGHN  
Special Agent  
FBI

Subscribed and sworn to before me on January 29, 2020



---

The Honorable PATRICIA L. COHEN  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the Facebook account(s) and/or user ID(s) **Cash Bandicoot (ID: 100001392692564)** that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company located at 1601 Willow Road, Menlo Park, CA 94025.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Facebook**

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f),

Facebook is required to disclose, from **10/01/2017 through 01/27/2020**, the following information to the government for the account(s) and user ID(s) listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- (c) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that account and user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (d) All “check ins” and other location information;
- (e) All IP logs, including all records of the IP addresses that logged into the account;
- (f) All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
- (g) All information about the Facebook pages that the account is or was a “fan” of;
- (h) All past and present lists of friends created by the account;
- (i) All information about the user’s access and use of Facebook Marketplace;
- (j) The types of service utilized by the user;
- (k) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (l) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (m) All records pertaining to communications between Facebook and any person regarding the user or the account and user ID, including contacts with support services and records of actions taken.

- (n) Any and all cookies associated with or used by any computer or web browser associated with the account, including the IP addresses, dates, and times associated with the recognition of any such cookie;
- (o) All records of Facebook searches performed by the account;
- (p) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- (q) All photos and videos uploaded by that account and user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
- (r) All location data associated with the account created, uploaded, or shared by the account;
- (s) All other records and contents of communications and messages made or received by the user, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests.

**Facebook is hereby ordered to disclose the above information to the United States within 14 days of the date of this warrant.**

## **II. Information to be seized by the United States**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1951 (hobbs act robbery), 2119 (carjacking), Section 924(c) (possession of a firearm in connection with a crime of violence), and 922, (unlawful possession of a firearm) by Darrin Cody from 10/01/2017 through

01/27/2020, including, for each account or user ID identified on Attachment A, information pertaining to the following matters:

- (a) Evidence of photographs and/or communications between Green/Frazier and others relating to the commission of the carjacking, possession and/or sale or trade of the carjacked vehicle, and/or possession and/or sale or trade of firearms. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (b) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (c) The identity of the person(s) who created or used the account(s) or user ID, including records that help reveal the whereabouts of such person(s).



**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO  
FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Facebook, and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Facebook. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Facebook, and they were made by Facebook as a regular practice; and

b. such records were generated by Facebook's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Facebook in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Facebook, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature